# (U) SIGINT Mission Strategic Plan FY2008-2013

3 October 2007 Release

[redacted]
[redacted] Signals Intelligence

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

# (U) BACKGROUND

(U//FOUO) America invests in intelligence programs to detect, and to provide full and timely answers to questions about, the hidden pursuits of persons, states, or organizations. In the case of signals intelligence (SIGINT), the expectation is that surveillance of targeted electronic signals and systems will yield insight that's worth the costly capabilities and operations needed to obtain it. For over 50 years, from World War II through the global war on terrorism, this investment has been justified, but the mission is still rightly judged by the answers it delivers. The implied business model is to position the mission to cover enough priority targets to ensure a steady stream of valued products and services for decision makers and other SIGINT consumers.

(U) This strategic plan seeks to maintain or enhance the mission's value in light of the challenges – and opportunities – of the unfolding network age. It frames and establishes several key aims and assigns responsibility for actions needed to attain them. At the highest level, success is defined as stable or improved responsiveness to customer needs, while doing best against the targets that matter most and avoiding strategic surprise.[1]

(U) The plan was developed through the on-line collaboration of over 250 SIGINT practitioners and partners, working within a framework created by the chief SIGINT strategist. It focuses on a small set of acts that should pay large dividends, and introduces data-driven processes to track progress, spot problems, and prompt adjustments. It's how we'll continue to modernize the way we prepare for, perform, and appraise SIGINT operations in a world in transformation.

# (U) DRIVERS

(S//REL) Since 2003 the intelligence community has been guided by a national intelligence priorities framework (NIPF) that maps customer needs into bands (A, B, and C) of successively lower concern. "Band A" topics include those strategic, asymmetric, and other threats that have the potential to greatly harm the U.S. or its interests. Within each topic, a 1-5 priority is assigned to specific geopolitical or non-state entities of interest, with 1 being the highest. Of course, not all intelligence questions are necessarily best, or even reasonably, probed by SIGINT means. Potential customers are asked to request SIGINT only when they can characterize its expected contribution as supplementary, substantial, key, or extraordinary.

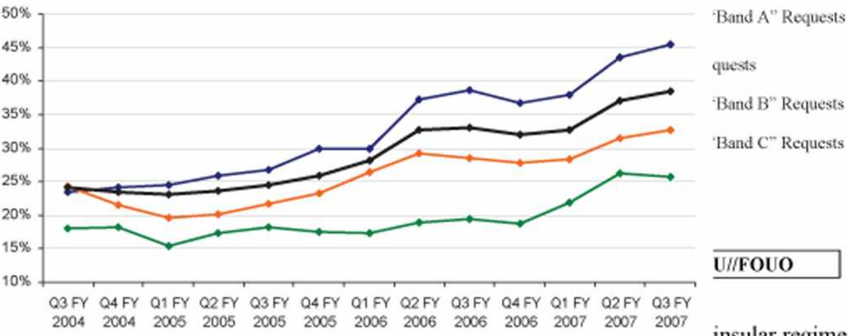
(S//REL) Since October of 2005, a national intelligence strategy has provided additional direction. Its five overarching mission objectives are to defeat terrorism, prevent and counter the spread of weapons of mass destruction, bolster the growth of democracy, penetrate hard targets, and anticipate developments of strategic concern. Of course, neither these nor the roster of "Band A" topics represent a radical shift from prior thinking. For several years, the SIGINT system has pursued these issues, intensifying efforts to harvest data from computers, Internet traffic, and other packetized communications in the process. As the chart shows, there has in

---

1 (U) As outlined in Appendix A, end-to-end performance will be judged by quantitative and qualitative analysis of customer requests and mission deliverables, and by authoritative customer surveys.

fact been significant growth in the percentage of customer questions, and especially high priority ones, that are being at least partially answered by serialized SIGINT reporting.[2]

(U) Percentage of Information Requests Addressed, Q3 FY04 to Q3 FY07




insular regimes often remains at a premium, as is information about asymmetric threats such as weapons of mass destruction, hostile cyber activities, and some terrorist organizations. Moreover, past gains are always under pressure from the relentless evolution of targets and technology.

(TS//SI//REL) For instance, as Internet routing and service nodes become more dispersed, some lucrative SIGINT chokepoints vanish and it takes more access points or over-the-net operations to maintain the same coverage. As strong cryptography is applied to identity management, software attestation, protecting data at rest, and securing network metadata, we must comparably expand cryptographic enabling, sensitive commercial partnerships, and cryptanalytic processing capabilities. As users become more mobile and more anonymous, we must introduce new association and pattern detection technology, lest targets of interest be lost or overlooked.

(S//SI//REL) At the same time, global modernization makes intelligence on economic, political, and other civil issues more valuable, and relevant targets tend to favor networks. Internet-centric activities such as e-commerce, e-voting, and on-net industrial and utility control beg to be mined, even as we expand existing operations against both public and private nets. Mounting interest in cyber security and the on-line aspects of crime and extremism also spur demand for network surveillance, as well as more interaction with atypical customers such as state and local governments, and tighter partnerships with consumers whose own target knowledge can help steer and interpret collection or whose operations can be "cued" by SIGINT.

(S//REL) Some efforts to recruit, train, and direct Islamic and other extremists are already entrusted to networks, and so will be many plans and acts of the PRC as it rises to be a near-peer competitor. Ruling institutions of even rogue states make some use of Internet technology, as do the scientists and proliferators with which they work. In fact, fewer and fewer targets of any stripe or location are far removed from a colleague, confidant, or confederate that's in the know and on the net.

---

2 (U) "Questions" are defined here as desired essential elements of information specified in standing COMINT or FISINT requirements. They're considered "addressed" when cited in serialized reporting issued during the quarter.

# (U) VISION, VECTORS, & VALUES

(U) Our mission is to answer questions about threatening activities that others mean to keep hidden. This is the essence of what we accomplish for the American people, whether we're supporting the global war on terrorism, infiltrating the leadership circles of strategic rivals or rogue states, or anticipating geopolitical and target technology trends.

(U//FOUO) Our vision, or aspiration, is to utterly master the foreign intelligence implications of networks and network technology. Even conservative people and institutions find themselves having to entrust their plans and operations to networks or else so limit their ability to acquire information, issue instructions, and move people, money, materiel, and ideas as to risk irrelevance. The mission must be planned, equipped, and executed for best effect, against the objectives that matter most, in this brave new digital world.

(U) At the heart of the task is the need to sense, and make sense of, systems, traffic, users, and various types and levels of organizations. This is a circular and fast moving process. New insight leads to better sensing, which leads to still greater insight, and so on – sometimes in months, but sometimes in minutes.

(S//SI//REL) Today, most of what we access goes unexplored or unexploited. Humans can neither follow network flows in real-time nor forge intelligence gold from an accumulation of isolated data points whose worth is only apparent when combined with one another and with what others may know. Our global sensors need to be able to think for themselves and talk to one another instantaneously. Our processing systems need to automatically find meaning in and across vast and dispersed data sets. Our analysts need new skills and new tools, and need to apply them in new ways, often in concert with customers. Our business processes need to promote data-driven decision-making and more disciplined end-to-end planning.

(U) This will not happen without leadership and the courage to ask if the practices and structures that serve us well today will continue to do so in the future. At the same time, some immutable values must continue to influence our daily choices and behavior. All military and civilian employees are called to commit to lawfulness, honesty, integrity, fairness, accountability, loyalty, collaboration, innovation, and learning. As we in the SIGINT mission grapple with the peculiar risks and rewards of the times and tasks at hand, a few implications of these commitments warrant special comment:

- (U) SIGINT professionals must hold the moral high ground, even as terrorists or dictators seek to exploit our freedoms. Some of our adversaries will say or do anything to advance their cause; we will not. All employees must have uncompromising devotion to personal and institutional integrity – doing the right thing, every time, regardless of how difficult it is.
- (U) SIGINT professionals must be honest with themselves, colleagues, superiors, and overseers. When something won't work, isn't working, hasn't worked, or went wrong, we need to say so, with respect, but also with unmistakable clarity. We then find a different way forward.
- (U) SIGINT professionals need to grow and prosper as mission assets *and* as individuals. We encourage career-long learning, periodic stretch assignments, and a balance between work and home life that honors duty to family, community, and self as well as to country.

# (U) KEY AIMS & ACTIONS

(U) We seek to maximize the SIGINT mission's value to the nation in the context of the intelligence priorities and technological realities of the network age. Fortunately, no matter what streams of operational and engineering initiatives – from the incremental to the transformational – are running their course at a particular time, a few core structures can channel them for best effect. The following goals are intended to do just that. As implementation of the plan proceeds, the responsibilities described below will be further decomposed into subtasks for various mission elements and levels. Ultimately, much of the daily work of the SIGINT enterprise will benefit, including the immediate mission imperatives presented in Appendix B.

(U//FOUO) **Goal 1**: Annually improve SIGINT on NIPF "priority 1" tasks and "Band A" topics in general, as measured by more even performance across topics and rising performance overall.[3]

**A.** (U) Responsibility and Accountability: Beginning in October 2007, the mission's Deputy Director for Customer Relationships (DDCR) will assess SIGINT mission performance against NIPF "Band A" tasks using methods outlined in Appendix A. *The DDCR will provide the mission's senior leaders with quarterly "Band A" performance reports and quarterly identification of un- or under-satisfied "Band A" tasks.*

**B.** (U//FOUO) Responsibility and Accountability: Beginning in FY08, the DDCR will lead the missions Deputy Directors for Analysis and Production (DDAP) and Data Acquisition (DDDA), and Associate Deputy Director for SIGINT Development (ADD SIGDEV) through joint reviews of un- or under-satisfied "Band A" tasks to find and address problems. *The DDCR will provide the SIGINT Director with quarterly improvement plans and progress reports, including concurrence, analysis, and commitments from the DDAP, DDDA, and ADD SIGDEV.*

**C.** (U//FOUO) Responsibility and Accountability: By April 2008, the DDDA will begin tracking the current and expected purpose and (using documented business rules) productivity of 1st, 2nd, and 3rd party SIGINT accesses.[4] *The DDDA will provide the SIGINT Director with quarterly comparisons of the "Band A" tasks given to, and the disposition and use of the resultant collection from, each access, highlighting un- or under-satisfied tasks.*

**D.** (U//FOUO) Responsibility and Accountability: Beginning in FY09, the DDDA will systematically reengineer, retire, or replace (directly or though a partner) chronically

---

[3] (U//FOUO) While performance against "Band A" topics is our benchmark, we will continue to work all high priority tasks, and lesser "Band B" and "Band C" issues when it's affordable and plays to our strengths.

[4] (U//FOUO) "Access" as used here refers to data sources that are at least partially funded via the collection and operations investment portfolio. The purpose or productivity of an access may relate to tipping, steering, or otherwise enabling other collectors, as opposed to collecting targeted information directly. Uniqueness and untapped potential are also factors to consider as is the expected contribution of an access in the event of a reasonably likely and significant future crisis or concern.

underperforming accesses. *The DDDA will annually provide the SIGINT Director with a multiyear "access enhancement" plan as part of the program build cycle.*

**E.** (U) Responsibility and Accountability: Beginning in FY08, the Agency's Chief Technology Officer (CTO) – with the full support of relevant collection, analysis, and customer engagement elements – will start to systematically instrument SIGINT tasking, ingestion, processing, analysis, and delivery systems to automatically tag data so that its source and subsequent processing and handling can be associated with some categorization of its ultimate use or intelligence value. *The CTO will provide the Agency's Senior Leadership with semi-annual reports on the percentage of data accessed that can be so associated.*

(U//FOUO) **Goal 2**: Field an analytic workforce that promptly and methodically discovers and exploits priority secrets entrusted to networks worldwide and helps customers turn this insight into significant national outcomes.

**A.** (U//FOUO) Responsibility and Accountability: Beginning with FY08, the CTO will enable improved information discovery by orchestrating annual increases in the proportion of newly acquired and archived data and metadata that can be readily searched and retrieved by analysts across the enterprise using standard workstations. *The CTO will develop baseline measures of accessible data, query times, and query difficulty, and provide the SIGINT Director with annual improvement reports, beginning at the end of FY08.*

**B.** (U//FOUO) Responsibility and Accountability: In FY08 and out, the NSA/CSS Senior Language and NSA/CSS Senior Intelligence Authorities will maintain a global training requirement for all cryptologic language and intelligence analysts performing various classes of missions and functions; will identify the types of learning activities that meet the requirement, based on current and projected needs and workforce statistics; and will provide data on organizational compliance to SIGINT mission and Agency leadership. *The NSA/CSS Senior Language and Intelligence Authorities and line managers of relevant organizations will ensure that at least 80% of all cryptologic intelligence and language analysts will engage in 160 hours of prescribed approved professional development every two years, and that at least 10% of language and intelligence analysts working the counterterrorism mission will be engaged in advanced or specialized training at any given time.*[5]

**C.** (U//FOUO) Responsibility and Accountability: Beginning in FY08, the DDCR and the DDAP will cultivate client-consultant relationships with more customers to facilitate new and more productive tasking and consumption of SIGINT products and services. *The DDAP will provide the SIGINT Director with an annual report on the number, disposition, and documented impact of analysts serving in full-time consultancy assignments.*

**D.** (C//REL) Responsibility and Accountability: Beginning in FY08, the DDAP will increase the practice of forward deploying analysts into customer workspaces to facilitate real-time analysis and iterative consultation where needed. *The DDAP will provide the SIGINT Director with quarterly summaries of the number and location of forward deployed analysts and their operational impact as assessed by customer surveys.*

**E.** (U//FOUO) Responsibility and Accountability: Beginning in FY08, the DDAP will systematically hand off mature analytic tasks to qualified partners when doing so increases

---

[5] (U) The latter is already a requirement of the National Counterterrorism Intelligence Plan.

the effectiveness or efficiency of the resources available to the U.S government and the SIGINT mission. *The DDAP will provide the SIGINT Director with an annual report on the tasks so "franchised" over the previous fiscal year, how any recovered resources were reemployed, and the customer impacts of both.*

(U) **Goal 3**: Annually increase the use of business cases to allocate pay and non-pay dollars and scarce skills for better returns on investment than alternative ways of using the same resources.[6]

***A.*** (U//FOUO) Responsibility and Accountability: Beginning in FY08, the chief SIGINT strategist will identify those skills that, for lack of critical mass, keep us from meaningfully migrating to new net centric tools and techniques, even if resources are adequate to expand existing types of collection, processing, or analysis operations. *Prior to each year's program build cycle, the chief SIGINT strategist will provide investment portfolio managers and the SIGINT mission's senior leadership with an annual list of work roles whose incumbents are to be considered "scarce resources" for business planning purposes.*

***B.*** (U) Responsibility and Accountability: Beginning in FY08, the DDCR and the ADD SIGDEV will fuse insight into technology and geopolitical trends and then clearly articulate the prioritized implications for the SIGINT mission. *Prior to each year's program build cycle, the DDCR and the ADD SIGDEV will provide investment portfolio managers with easily consumable and actionable planning guidance aimed at avoiding technological or strategic surprise and optimally ordering potential investments.*

***C.*** (U) Responsibility and Accountability: Beginning with the FY10-15 program build, the Collection & Operations, Processing & Exploitation, Analysis & Production, and Mission Management investment portfolio managers will revalidate or construct new business cases covering ever larger proportions of their pay and non-pay submissions. *As part of each year's program build cycle, each of the four investment managers will submit business cases to the SIGINT Director covering more of their portfolio than previous budgets.*

# (U) INVESTMENTS

(U) The national intelligence program allocates pay and non-pay dollars to the SIGINT mission through seven investment portfolios. As discussed below, the work of each must be tailored for success in a changing world. Ultimately, desired customer outcomes demand certain operational concepts and functions. These require sets of personnel and technical capabilities and supporting infrastructure, all playing the right role at the right time as scripted by system engineering.

**(U) Collection and Operations**

(TS//SI//REL) Historically, we've arrayed independent accesses against various streams of point-to-point communications. As we shift from intercepting links to exploiting networks though, multiple collection platforms must be engineered and outfitted to work in concert, and often in real-time. Vast quantities of message externals and other network metadata must be harvested,

[6] (U) Such business cases should take into account national priorities, geopolitical and technology forecasts, mission assessment data, and defensible cost information.

often via bulk "midpoint" collection of global backbones. Vendors and service providers must also be leveraged to obtain metadata and other targeting and vulnerability information, as well as traffic. "Endpoint" operations must expand, to retrieve more targeted data directly and to alter routing or encryption for the benefit of passive sensors.

(S//SI//REL) Midpoint collectors will still be used to acquire content (and not just metadata), but with less success and at greater cost as traffic volumes and velocities rise. Mobile and tactical systems, covert and clandestine programs, and overhead assets will continue to perform their specialized tasks until the spread of network technology offers a better play, and will be modernized as the mission requires or when automation or new technology can significantly reduce long-term manpower or life-cycle support costs. Endpoint methods will be used for more ELINT and FIS tasks, gathering data on some weapons or emitters before they're deployed.[7]

**(U) Processing and Exploitation**

(S//SI//REL) If collection operations around the globe are to work in tandem in real-time, then the processing and exploitation fabric of the SIGINT system must provide for distributed storage and robust messaging. Fast, flexible, front-end processors must spot targets based on patterns, events, or metadata rather than pre-defined selectors or brute force scanning of content. High performance computing systems must extract meaning from huge data sets and to negate data encryption and computer access controls.

(S//SI//REL) New developments will stress standardized interfaces that let diverse applications share infrastructure, and will favor automation and off-the-shelf technology over manual processes and point solutions. New SIGINT system architectures will de-couple event detection from follow-on reaction and processing, so that applications can be added or deleted with little impact to ongoing operations and so that sensors and processors can serve many tasks rather than one operational stovepipe. All this – and increased use of remotely configurable commercial hardware – will also cut the time needed to retool or refocus technical infrastructure as customer needs, target behaviors, or technical constraints change; they'll reduce life-cycle costs as well.

**(U) Analysis and Production**

(S//SI//REL) In the aftermath of the digital revolution, powerful analytics and empowered analysts are how we discover targets and their secrets and how we harness our technical capabilities to our customers' missions. Advances in collection and processing must let us flag events of interest as they happen, accumulate far more context-rich metadata, and collate targeted communications and transactions across accesses. To take advantage of this, analysts must have new tasking, association, and presentation tools, and larger and more adaptable storage and retrieval systems. Fortunately, information management and mining is central to the Internet age and next-generation analytics can employ many commercial products and practices.

(S//REL) Looking forward, we will continue to devote more analysts to exploiting digital network intelligence and to working problems related to counter-terrorism, counter-proliferation, China, Iran, and the Middle East, aggressively investing in the necessary tools and training, and "franchising" some mature missions to qualified partners. We will deemphasize the traditional concept of a SIGINT storefront (requirements in/reporting out) in favor of having far more analysts working physically or virtually within the missions that they support. They will act more as a consultancy than a simple data source, helping shape customer plans to reflect the "art

[7] (U//FOUO) Some characterization of actual emitters in real world operation may still, however, be necessary.

of the possible" and giving each customer's own analytic workforce the power and knowledge to reap, rather than just consume, SIGINT.

**(U) Mission Management**

(U//FOUO) To optimize ever more complex, fast-moving, cross-access operations, we must introduce intelligent agent technology that automatically updates tasking and status as it interacts with technical infrastructure, visualization tools, and authoritative databases. To prevent strategic surprise, we must track geopolitical and technology trends to identify potential gaps and mitigate them before mission performance degrades. To accommodate an increased fusion of SIGINT analysis with customer activities, we must develop new mission management tools that capture and handle a freer flow of interactions and new forms of support. To pave the way for more meaningful productivity estimates and more enlightened investment decisions, we must instrument collection, processing, and dissemination systems so that sources can be linked through analysis to customer outcomes.

**(U) Research**

(S//SI//REL) Our ability to master global networks and handle previously unimagined volumes of raw data from both passive and active collection will depend in large part on successful research. Requirements include ever more powerful methods of knowledge discovery and management, highly capable software implants and mobile agents, optimal distributed storage arrangements, and advanced analytic algorithms. Underpinning all this must be high productivity computing systems and world-leading cryptanalytic talent that can both cope with pervasive hard encryption and find and exploit meaning in large data sets generally. Researchers must also break new ground in the area of enterprise security management if we're to fully realize a more interconnected, distributed, and autonomous SIGINT operations fabric and geographically dispersed analytic collaboration.

**(U) Enterprise IT and Enterprise Management**

(U//FOUO) New operational strategies and capabilities can't deliver on their promises without the right military, civilian, and contractor workforce, a modernized enterprise information technology infrastructure, and an assured 21$^{st}$ century physical plant. The quantity and quality of language analysts, intelligence analysts, mathematicians, and computer network exploitation specialists are priorities, as is rebuilding the acquisition, system engineering, and business/project management workforce. Another imperative is modernizing enterprise networks, platforms, and services; this effort ranges from bandwidth expansion, to server consolidation and refresh, to introducing user tokens and other information assurance measures. A third is dealing with long-deferred real property maintenance and the mitigation of long-simmering power, space, and cooling shortfalls.

# (U) APPENDIX A: Assessing Overall Performance

(U//FOUO) Customers request SIGINT by specifying the "essential elements of information" (EEIs) that they want to uncover. The National Intelligence Priorities Framework (NIPF) maps each EEI into one of three bands (A, B, or C) of successively decreasing concern according to general topic, and assigns a 1-5 priority based on the combination of the topic and specific geopolitical or non-state entity involved. Responsive SIGINT is delivered in several forms, but serialized reporting dominates, and so one indicator of end-to-end mission performance is the percentage of requested EEIs for which at least some responsive reporting is provided (i.e., *the EEI citation rate)*.

(U//FOUO) At a macro-level, the overall citation rate for "Band A" EEIs should be greater than that for "Band B," which in turn should exceed that for "Band C". Beyond that, performance against each "Band A" topic is also weighed in accordance with the following first-order rules. Performance is *poor* if a "Band A" topic's rate doesn't even exceed the overall "Band B" rate. Performance is *weak* if a topic's rate is above the overall "Band B" rate, but less than the overall "Band A" rate. Performance is *fair or good* if a topic's rate is at or above the overall "Band A" rate, with the latter also requiring that the rate for the topic's "priority 1" EEIs be higher than that for the topic's EEIs generally.

(U) Citation rates reflect only the existence of responsive SIGINT, and not its impact. Moreover, they don't directly account for requests that are addressed entirely by other than serialized reporting, and they can be skewed by careless recordkeeping or differences in granularity between EEIs. Therefore, quarterly citation rate assessments are complemented with two broader, more subjective, and more manpower intensive views of customer outcomes and satisfaction.

(U//FOUO) The first is a quarterly, manual assessment of performance against each NIPF "Band A" topic that includes niche interactions that don't involve EEIs as well as deliverables beyond serialized reporting. Performance is graded on the extent to which records show that responsive information was pushed to or pulled by a customer, *and* sampling suggests that the records that tie deliverables to requests are accurate, *and* sampling suggests that the information delivered was germane vice just tangential. Performance is *poor* if responsiveness is well below average (relative to that for "Band A" tasks as a whole), *weak* if responsiveness is somewhat below average, *fair* if responsiveness is average or better, and *good* if responsiveness overall is average or better *and* is better still against high priorities.

(U//FOUO) The second is a quarterly survey of roughly 20 intelligence consumers, specified by position based on their ability to speak knowledgably and authoritatively about the SIGINT contributions to key civil or military customers. Those solicited represent the unified combatant commands and the Joint Staff; the Departments of State, Treasury, Commerce, Energy, and Homeland Security; the Central Intelligence and Defense Intelligence Agencies, the Federal Bureau of Investigation; the Drug Enforcement Administration; the National Counterterrorism Center; the U.S. Trade Representative; and the White House Situation Room.

# (U) APPENDIX B: IMMEDIATE IMPERATIVES

- (S//REL) Gain more pervasive and persistent insight into al-Qa'ida, al-Qa'ida affiliates, Hezbollah, and other terrorist targets, despite their increasingly aggressive COMSEC practices.
- (S//REL) Infiltrate the most secret communications and data of the leadership, military, and security bureaus of Iran, North Korea, China, and similar targets of high concern.
- (U) Better define and pursue immediate, near-term, and strategic mission management.
- (U//FOUO) Optimize SIGINT discovery to find and follow targets, refine their prosecution, and anticipate their shifts.
- (U) Identify and plan for geopolitical and technology trends.
- (U//FOUO) Introduce productized net-centric capabilities into mainstream SIGINT operations on a scale that produces significant dividends in the counterterrorism arena and elsewhere.